USOE Information Technology Security Plan

1. Introduction.

This document, along with appendices, is a detailed description of security practices within the USOE. It is meant to be a dynamic plan that will, at least in part, be shared will all staff through appropriate training and media. Some of the information presented in this plan was borrowed from public sources, most notably the National Center for Education Statistics (NCES) web site (http://nces.ed.gov).

2. Security Management Processes

At the present time oversight of security at the USOE is guided by a designated IT security officer who shares security responsibilities with other technical staff. Areas in which implementation is not complete at the present time are: training, intrusion detection and in some areas rigorous software quality assurance. Those the roles of those responsible for the implementation of security policy include:

2.1. Ensure the secure installation of all systems.

2.2. Monitor system use to help detect security breaches, intrusions and violations.

2.3. Coordinate and maintain security software services such as antivirus, spyware detection and data encryption.

2.4. Communicate to staff that protecting the system is not only in the organization's interests, but also in the best interest of users.

2.5. Increase staff awareness of security issues.

2.6. Provide for appropriate mandatory staff security training

All new and existing employees be required to participate in a security course and pass a quiz once each school year. See section 8.3.

2.7. Monitor user activity to assess security implementation.

2.8. Be inclusive when building a security and contingency planning team by including:

2.8.1. Key policy-makers

2.8.2. The security manager

2.8.3. Building management

2.8.4. Technical support

2.8.5. End-users

2.8.6. Other representative staff

2.8.7. Local authorities

2.8.8. Key outside contacts (e.g., contractors and suppliers)

3. Physical Security

3.1. Building (The responsibility of the building security coordinator)

3.1.1. Protected by a fire detection system.

3.1.2. Building access. All external doors, but one, are locked at all times and require an electronic key for entry.

3.1.3. Onsite Guard. Only one door is unlocked from the outside during business hours (7:00 AM to 5:30 PM) and that is monitored by a guard.

3.1.4. Surveillance cameras. The guard, during business hours, also has access to external and internal surveillance cameras.

3.1.5. Internal Building Access. After business hours all sections of the building except the main first floor hallway are also secured. The computer services section is in the basement of the building to which access is denied to all but authorized employees during non-work hours.

3.1.6. Employee Building Access. Employees are screened and given off hours access to appropriate areas of the building depending on their roles. All employees must wear USOE badges at all times within the building.

3.2. Network Room (Responsibility of the building security coordinator and the IT security officer)

3.2.1. Water damage. All hardware and wiring is elevated off floors in racks or trays. The fire prevention sprinkler system is dry loaded (no water immediately overhead), meaning that water can only be released if an actual fire triggers a valve behind the actual sprinkler system.

3.2.2. An automatic power cutoff switch activates by detection of moisture or smoke or heat.

3.2.3. Physical Access. Only one inconspicuous door provides access to the network room and that door is secure by a key pad lock.

3.2.4. Electrical Overloads. Hardware VA rating and totals are assessed to make sure any one circuit is not being overloaded. When needed, more circuits are added to the network room. Total volt-amps and wattage is kept at 60% or lower of the maximum capacity of a circuit.

3.2.5. Earthquakes. Individual devices are securely attached to racks and racks are anchored to the ceiling, floor or other secured racks.

3.2.6. Power Backup. All network room hardware is on a managed UPS system. That system is on a diesel powered generator backup power system which is able to supply emergency power to the building for at least 24 hours.

3.2.7. Temperature control. If the temperature climbs past a predefined maximum, currently 75 degrees Fahrenheit, automatic alarms are trigger and automatic phone calls are made to

key USOE computer services staff and state DFCM (Division of Facilities and Construction Maintenance).

3.2.8. The HV/AC system is also on diesel powered generator backup power. When power is lost to the building the air conditioning continues to function for up to 24 hours by running off the diesel generated power. Without continuous air conditioning the heat generated by the electronic equipment would quickly cause the temperatures to rise to levels which would be hazardous to the electrical equipment.

3.2.9. The network/server room has and emergency power-off button for use in case of emergency that shuts done hardware in an predictable manner.

4. Data/Information Security & Privacy/Confidentiality (also see: **Data Access Security and** Appendix A for more details about privacy, FERPA and GRAMA at the USOE)

4.1. Policy Statement. The Utah State Office of Education (USOE) makes every effort to abide by all applicable State and Federal guidelines, policies, regulations, statutes, and procedures pertaining to the confidentiality and privacy or data. The USOE does not permit access to, or the disclosure of, student records or personally identifiable information contained therein (other than directory information) except for purposes authorized under the Family Educational Rights and Privacy Act (FERPA). FERPA assures students that their records are protected from unauthorized access or disclosure and requires a clear understanding of the type of information that can be released without an individual's consent. The USOE also does not permit unauthorized access to, or the disclosure of educator and employee records or personally identifiable information contained therein.

As a result, it is important to handle all confidential information with discretion, safeguarding it when in use, storing it safely, updating or disposing of it properly, and discussing it only with those who have a need to know for a legitimate business reason. In most cases, data of a personally identifiable nature shall remain secure from public disclosure (release to third parties) without specific permission from the individual to whom those data apply.

4.2. Policy Purpose. This policy establishes the procedures and protocols for collecting, maintaining, disclosing, and disposing of education records containing personally identifiable information about students and educators or any other individual for whom the USOE maintains data. It is intended to be consistent with the disclosure provisions of the FERPA. All users of USOE information systems must follow the practices outlined below.

4.3. Definitions.

4.3.1. Directory Information can mean any of the following:
- 4.3.1.1. Student's name, address, telephone listing, and date of birth
- 4.3.1.2. Parent or lawful custodian's name, address, and telephone listing
- 4.3.1.3. Grade level classification
- 4.3.1.4. Dates of attendance, dates of enrollment, withdrawal, re-entry
- 4.3.1.5. Diplomas, certificates, awards and honors received
- 4.3.1.6. Most recent previous educational institution attended

4.3.2. "Disclose" or "Disclosure" means to permit access to, or to release, transfer, or otherwise communicate, personally-identifiable information contained in education records to any

party, by any means, including oral, written, or electronic means.

4.3.3. "Education Records" means any information or data recorded in any medium, including but not limited to handwriting, print, tapes, film, microfilm, and microfiche, which contain information directly related to a student and which are maintained by USOE or any employee, agent, or contractor of USOE.

4.3.4. "Maintain the Confidentiality" means to preserve the secrecy of information by not disclosing the information

4.3.5. "Personally-identifiable" means data or a record that includes any of the following:

4.3.5.1. The name of a student, the student's parent or other family member

4.3.5.2. The address of the student

4.3.5.3. A personal identifier, such as the student's social security number or an assigned student number

4.3.5.4. A list of personal characteristics which makes the student's identity easily traceable

4.3.5.5. Other information which makes the student's identity easily traceable

4.3.6. "Security" means technical procedures that are implemented to ensure that records are not lost, stolen, vandalized, illegally accessed, or improperly disclosed.

4.3.7. "Student" means any person who is or has attended public or accredited nonpublic school and for whom USOE maintains education records or personally-identifiable information

4.3.8. “Educator” means someone who is or has been employee by a Utah public school or has applied for a Utah educator credential.

4.4. Information to be Maintained

The USOE collects and maintains personally identifiable information from education records of Utah students, to include

4.4.1. Personal data which identify each student. These data may include, but are not limited to, name, student identification number, address, race/ethnicity, gender, date of birth, place of birth ,social security number (only in special cases), name and address of parent or lawful custodian

4.4.2. Attendance and other pupil accounting data

4.4.3. Data regarding student progress, including grade level completed, school attended, academic work completed, and date of graduation

4.4.4. Standardized test scores including CRTs, UBSCT, NRTs and UALPA.

4.4.5. Data regarding eligibility for special education and special education services provided to the student.

4.4.6. Data regarding eligibility for other compensatory programs and special program services provided to the student.

4.4.7. Professional Educator data including outcomes of background checks, education and teaching history and any disciplinary measures.

4.4.8. SIS and Fiscal data for hosted districts.

4.5. Practices to Maintain the Confidentiality of Student Information

The USOE utilizes various procedures and security measures to ensure the confidentiality of student records. These procedures shall include assignment of a unique identifier to each student, restricted access to data, and statistical cutoff procedures (not reporting aggregate measures of small groups of student subgroups).

4.5.1. Unique Student IDs are assigned to each Utah student. The Student ID is computer generated and contains no embedded meaning. After being checked for duplicates, it is permanently assigned.

4.5.2. Security protocols are designed and implemented by the USOE. They limit who has access to the data and for what purposes.

4.5.3. The USOE has statistical cutoff procedures (not reporting aggregate measures of small groups of student subgroups) to ensure that confidentiality is maintained. For example, if there are less than ten students in a give racial group within a school, that group's average score on a standardized test would not be publicly reported.

4.5.4. All USOE personnel collecting or using personally-identifiable student information are provided instruction regarding procedures adopted in accordance with this policy. They are required to sign a confidentiality agreement. (See appendix M).

4.5.5. The USOE maintains a current listing of agency personnel who have access to personally-identifiable student information. Generally, inclusion in this list is limited to: data stewards, developers and data base administrators. These personnel will be responsible for any extracted and disseminated data. USOE databases can log such activity.

4.6. Individual Employee Rules

4.6.1. Data originated or stored on agency computer systems are USOE property. Employees will access only data that are required for their job. Employees will not make or permit unauthorized use of any USOE data. They will not seek personal or financial benefit or allow others to benefit personally or financially by knowledge of any data that has come to them by virtue of their work assignment.

4.6.2. Employees will not release agency data in any format except as required in the performance of their job. Employees will not remove, electronically or printed, an official record or report, or copy of one, from the office where it is maintained, except as may be necessary in the performance of their job. They will not exhibit or divulge the contents of any record or report to any unauthorized person except in the conduct of their work

assignment and in accordance with USOE policies and procedures.

4.6.3. Employees will not share their computer login information, including password(s) with others or leave their written password(s) in a place that could be accessible by others. If a user has reason to believe others have learned their password(s), they will report the problem to their supervisor and will take appropriate action to have the password(s) reset. Employees will not attempt to use the logins and passwords of others, nor allow their logins and passwords to be used by others. All employees are responsible for anything done under their account and are subject to all appropriate corrective and/or disciplinary actions.

4.6.4. Employees will maintain the security of all USOE data in their possession or to which they have access by protecting computer media, forms and printouts from unauthorized access and will dispose of them in a safe manner. Further, employees will not leave their PC signed on when unauthorized people could access it, will change their password(s) on a regular basis, and will take other precautionary measures necessary to protect and secure, confidential, or sensitive data.

4.6.5. Employees will not store any sensitive data including Social Security Numbers, credit card numbers, or student identifiable data on any removable media or computer except on a properly secured server.

4.6.6. Routine scans of all local user storage content on desktops and laptops is not done at USOE nor is it done at other Utah agencies. However, any local storage will be thoroughly scanned at the request of the HR director. The USOE follows numerous other security policies and procedures, including scanning for social security numbers on servers as described in this security plan. This also includes random scanning for suspicious behavior, events, and unapproved, illegal or high risk software.

Based on virus reports, intrusion detection and prevention alerts, unusual traffic, high bandwidth usage, and zone Administrators' reports, a given machine may become suspect. Some or all of these conditions may be cause for the scanning and/or monitoring of a given machine. Such scanning and monitory may include, among others, scanning for: social security numbers, individually identifiable data, viruses, hacking software and other unauthorized software.

4.6.7. Users are only permitted to have agency approved and purchased software installed on their machines. This includes web and windows applications.

4.6.8.

Security violations may entail taking the user's machine and "wiping" it to make sure it's clean. Mandatory computer and security training are in place to avoid these situations.

Computer Services will work closely with Human Resources in enforcement activities. However, a clear line is drawn between each party's role in the process. While Computer Services may discover and report a violation/infraction, it is up to Human Resources to do the actual enforcement

Actions to be taken for violations will be determined by following the guidelines described in Appendix Q.

4.7. Disclosure of Data for Research

The USOE may disclose confidential, personally identifiable information of students to organizations for research and analysis purposes to improve instruction in public schools. Any such disclosure shall be made only if the following requirements are met.

4.7.1. The conditions in FERPA regulation 34 CFR 99.31(a)(6) are met. (See Appendix A).

4.7.2. The research being done has been commissioned by the Utah State Board of Education. In some cases personally identifiable data may be provided the researcher/contractor but only in a secure manner.

4.7.3. Those not commissioned but desiring data must use the publicly available data on USOE Websites or request the researcher data disk that is provided by Computer Services. This generic data disk will developed each year and available upon request.

4.7.4. The recipient organization has signed the Researcher Confidentiality and Use Agreement Regarding Microdata. (See Appendix R).

4.8. Record of Access

The USOE maintains a record which indicates the name of any individual or organization external to USOE that requests and is allowed access to students' educational records. The record of access also indicates the interest such person or organization had in obtaining the information, as well as the date the requested data were disclosed. Agency section data stewards maintain such records.

4.9. Other Important privacy and confidentiality needs. Besides data governed by FERPA, the USOE is also responsible for providing controls over processes and procedures around educator licensing data, rehabilitation systems and records as well as school funding, budgeting and financing records and systems. Personally identifiable data in these datasets will also be maintained in a confidential and secure manner.

4.10. Data/Information Integrity (Preventing Unauthorized Creation, Modification, or Deletion of Information):

4.10.1. USOE staff never sends sensitive information as in e-mails

4.10.2. All data are to be encrypted before it leaves a server or workstation.

4.10.3. Secure, encrypted FTP and SSL services are always used when transmitting data to and from district facing applications and agency databases.

4.10.4. All data encryption devices and keys are to be physically protected. They must be stored away from the computer.

4.10.5. All staff are to be informed that all messages sent with or over the organization's computers belong to the organization and therefore subject to monitoring.

4.10.6. The receiver's authenticity must be verified before sending any USOE data or information. Everyone sending data outside the agency must ensure that users on the receiving end are

who they represent themselves to be by verifying: 1) Something they should know; a password or encryption key (this is the least expensive measure but also the least secure) or 2) Something they should have-for example, an electronic keycard or smart card.

4.10.7. Likewise, all data senders need to consider setting up pre-arranged transmission times with regular information trading partners: If you expect transmissions from your trading partners at specific times and suddenly find yourself receiving a message at a different time, you'll know to scrutinize that message more closely.

4.10.8. Likewise everyone must maintain security when shipping and receiving materials: When sending sensitive information through the mail, or by messenger or courier, require that all outside service providers meet or exceed your security requirements.

4.11. Practice the following safe data storage:

4.11.1. Backup files require appropriate levels of security as do the master files (e.g., if the original file is confidential, so is its backup).

4.11.2. Clearly label disks, tapes, containers, cabinets, and other storage devices: Contents and sensitivity should be prominently marked so that there is less chance of mistaken identity.

4.11.3. Never store sensitive data/information in such a way that it co-mingles with other data on floppy disks or other removable data storage media.

4.11.4. Information, programs, and other data should be entered into, or exported from the system only through acceptable channels and by staff with appropriate clearance and technical knowledge.

4.11.5. Write-protection should be used to limit accidental or malicious modification of files. Note that while write-protection is effective against some viruses, it is by no means adequate virus protection in itself.

4.11.6. Any staff must promptly notify the system administrator/security manager when data are, or are suspected of being, lost or damaged. This includes all stolen computing devices regardless of the data stored locally. Non-compliance will result in appropriate corrective and/or disciplinary actions.

4.12. Dispose of Information in a Timely and Thorough Manner:

4.12.1. Follow all USOE and State of Utah retention schedules for specific information or data sets.

4.12.2. Mark files to indicate the contents, their expected life cycle, and appropriate destruction dates.

4.12.3. Before discarding or surplusing obsolete or old media, it will be scrubbed or overwritten to make data recovery impossible. CD ROMs will be physically shredded.

4.12.4. Consider degaussing (a technique to erase information on a magnetic media by introducing it to a stronger magnetic field) as an erasure option.

4.12.5. Burn, shred, or otherwise physically destroy storage media (e.g., paper) that cannot be effectively overwritten or degaussed or scrubbed.

4.13. Data Availability:

Where data access is permissible the USOE must prevent any unauthorized delay or denial of information to qualified parties. Strict adherence must be given to FERPA and GRAMA at all times.

4.14. Law Enforcement Notification of Security Breaches or Unacceptable Behavior.

If any of the following are discovered on the USOE network, in consultation with USOE legal staff, appropriate law enforcement officials must be notified.

4.14.1. Child pornography
4.14.2. Attempts to solicit a minor
4.14.3. Death threats
4.14.4. Disclosure of Social Security Numbers
4.14.5. Disclosure of credit card numbers or other personal financial numbers

5. Software Security

5.1. Software installation.

Only network administrators and power users (see Appendix B) have rights to install or otherwise add software to any server, desktop or notebook system. Power users must sign a use agreement and receive special network training. (see Appendix B and Appendix C).

5.2. Storage of master copies.

Master copies of all software, licenses and documentation are retained in a secure location A database of licenses is maintained along with expiration and renewal schedules.

5.3. Approved Software.

Only USOE Computer Services approved and purchased or otherwise provided software that is installed by USOE network staff or USOE power users may be used on USOE machines. USOE Computer Services will only support and allow to connect to desktops and laptops PDAs and smart phones with Windows mobile operating systems. See Appendices M and N.

5.4. Non-Computer Services approved and purchased software.

Before permission is given to a power user for the installation of any non-CS approved software the user must submit a written request describing the nature of such software and the purpose for which it is to be installed.

5.5. Monitoring of software.

To counter possible copyright infringements caused by unlicensed software on organizational equipment that puts the entire organization at risk for fines and other penalties stemming from copyright violations, software inventories are done on a regular basis. These comprehensive network-wide inventories will include the: the product, name of the manufacturer, version

number, and the computer on which he software is installed. This inventory will be reconciled against the Computer Services software license inventory to verify that no unlicensed software or software for which the USOE has inadequate licenses is installed anywhere on the system.

5.6. Regulate Software Development and Changes:

5.6.1. Software development life cycle. All custom software is developed following a prescribed software development life cycle. (See Appendix E)

5.6.2. Authorization of software changes. Before anyone modifies or creates any software, a formal, written change request (see Appendix F) must be submitted to the IT director or an IT manager. Such requests must be signed by a section director or associate superintendent and result in an audit trail of artifacts and events as the request is processed.

5.6.3. Design Reviews. Continued feedback is expected from users during the software development process to ensure that the new or changed software will satisfy functional specifications and security requirements.

5.6.4. Production vs. Development Copies. To avoid putting active applications and files at risk all new development is done in a separate development/testing environment with separate test networks and servers were applicable. Once the modified or new copy/version of the software is thoroughly tested by the software development staff and prospective end-users, then and only then will it be deployed to the production or "live" environment.

5.6.5. Program review. Before new or changed programs are put into production the code changes are reviewed by at least one other person who understands the change request that initiated the new or changed code. This step precedes actually testing and is just one step in the quality assurance/quality control process.

5.6.6. Vulnerability checking: As much as possible program code should also be reviewed and tested for potential vulnerabilities such as buffer overflows and SQL injection attacks that would make it susceptible to various software exploits.

5.6.7. Master files. Master files of all developed software are maintained independently of the development staff: Software belongs to the organization, not the programmer. All original copies are controlled and the organization clearly guarantees this ownership. It is required that any new or modified software is tested rigorously and certified as fully operational before releasing it for general use.

5.6.8. Required documentation. For all new or revised programming, requisite documentation includes among others: the name of the developer, the name of the system, the modules/objects impacted, programming languages/technologies, the development/change dates, nature of the revision, the revision number etc.

5.6.9. Public programs: If software downloaded from the Internet must be used with sensitive information, be sure that it has not been tampered with by checking for a digital signature to verify its authenticity. See section 5.3.

5.6.10. Software Verification: Before putting the software into operation, verify that all software user functions are working properly. Check that new software meets anticipated user needs, current system requirements, and all organizational security standards. This

recommendation is also applicable when upgrading software.

5.6.11. Before installing new software or software upgrades: Copies of latest data files must be used for testing until the new software or upgrade is proven to be running properly.

5.6.12. Application software testing: Developers must never risk using live data with newly installed software. They must always run sample files and/or copies of non-sensitive files through the software to verify software's integrity and proper functioning.

5.6.13. Test machine isolation: Initial software testing should occur on test machines and a test network if at all possible. By maintaining a separate test environment, the entire system is not at risk if the software malfunctions.

5.6.14. No test machines will be granted general access from the Internet.

5.6.15. No test machines will be turned into production systems without being properly wiped first. No test server should ever go straight to production. There must be a test server and a production server. Test machines by nature are insecure and full of holes.

5.6.16. Parallel software testing: Run old software at the same time and with the same data as the new software. It should be confirmed that the new versions of the software must generate the same results as the existing system.

5.6.17. Backup of Custom Software: Like all other data on USOE servers, all custom developed software, including commercial software that has been modified with permission, is backed up on a predefined schedule. See backup plan in section 6.4.

6. Data Access Security (Data/Information Security & Privacy/Confidentiality)

While the vast majority of system users are trustworthy, there are occasional computing accidents. Most system problems are the result of human error. By instituting security procedures, the organization protects not only the system and its information, but also each user who could at some point unintentionally damage or expose a valued or confidential file.

6.1. Passwords:

After an independent audit of the USOE it was recommended that these actions be taken to improve security. The majority of the old passwords in the password database were cracked within 3 seconds.

6.1.1. All passwords be at least eight characters in length (ten or more is preferable).

6.1.2. No passwords are permitted that are words, names, dates, or other commonly expected formats.

6.1.3. Passwords should not reflect or identify the account owner (e.g., no birthdates, initials, or names of pets).

6.1.4. The password character string must contain one character from three of these four character types:

6.1.4.1. Uppercase letters

6.1.4.2. Lowercase letters

6.1.4.3. Numerals

6.1.4.4. Non-alphanumeric characters such as: (, . ; : * % &)

6.1.5. All users are forced to change passwords at least once every 90 days.

6.1.6. No users may share passwords.

6.1.7. Unsecured storage of personal passwords is forbidden (e.g., they should not be written on a Post-It™ note and taped to the side of a monitor).

6.1.8. A password may never be used as part of an e-mail message.

6.1.9. Users should be warned not to type their password when someone may be watching.

6.1.10. When developing software mask password display on the monitor when users type it in.

6.1.11. Remind users that it is easy to change passwords if they think that theirs may have been compromised.

6.1.12. No new password may be the same as an old password unless at least four other unique passwords have been used in between.

6.1.13. Users are discouraged from using the same password for two or more systems.

6.1.14. There have been questions about people wanting to keep their passwords the same across multiple systems such as: BASE, CACTUS, local network, PATI, AIMS, and IRIS. This is not a recommended practice. If your password were the same across multiple systems then a hacker who cracks one password would be able to access all of the other systems as well.

6.1.15. Mainframe passwords must also start with a letter, no special characters are allowed and all letters must be lowercase. Examples of passwords that will work are: syracuse1, and gr8dane.

6.2. Remote Access: All users must abide by a strict network access policy (see Appendix H) that governs attachment of individual computers both at home and at the workplace. This policy applies to both desktop and notebooks as well as PDA and smart phones.

6.3. Walk-in/Guest users:

Any walk-in or guest user must abide by the policies set forth above. Guest users may connect to a wireless network that is isolated from the USOE domain.

6.4. VNP Connections:

All connections made through VPN (Virtual Private Networking) by elecommuters or wireless users within the building must be made through agency owned and maintained machines. These machines will be allowed access only through a public/private key exchange.

6.5. Remote Access Monitoring:

Staff must be reminded that remote access is particularly subject to monitoring activities. Increased risk requires increased vigilance.

6.6. Message Authentication:

Use software that requires "message authentication" in addition to "user authentication": Even if a user can provide the right password, each message sent and received must have its delivery verified to ensure that an unauthorized user didn't interrupt the transmission.

6.7. Social Engineering:

No one will ever legitimately ask you for your password, inspect you machine for devices attached to your USB ports or added to your keyboard, etc. If you see any strange machine or device hooked to network or laying around how to report it, how to handle phone calls asking for information, etc.

6.8. Terminated Employees:

Computer Services must be immediately notified of the pending termination or position change of any employee regardless of the reason. Reinstatement of terminated employee files must be approved by an Associate Superintendent. See Appendix P.

7. Network Security:

An "access node" is a point on a network through which you can access the system. If even one such point is left unsecured, then the entire system is at risk. All modular jacks and wireless base stations represent potential nodes to which a computing device could be attached.

7.1. Protection of cables and wires:

All cabling and wires should be protected as much as possible. This means they should reside in trays in cubicles or within walls or ceilings. If a sophisticated intruder can access a span of cable that is used as a connector between pieces of equipment, he or she may be able to access the entire system.

7.2. Boot secured servers:

Secure all servers so they cannot be booted from removable devices or their BIOSs altered with administrative access.

7.3. Screen savers:

Screen savers with mandatory locking features must be installed on all user machines to prevent information from being read by anyone who happens to be walking past the display monitor. They should be set to activate after no more than 30 minutes on inactivity. All users are instructed to manually lock keyboard when moving away from their computers from any length of time.

7.4. Firewalls:

Firewalls are installed at all external access points: Only trusted (authenticated) messages can pass into the internal network from the outside. Only predefined ports may be opened.

7.5. Intrusion detection:

In conjunction with its firewalls, the USOE maintains intrusion prevention/detection software running in an appropriate configuration within the firewall's demilitarized zone (DMZ). Such software will detect possible intrusions, hacks, or other exploits aimed at compromising the system.

7.6. Modems:

Only in very special cases should a modem be necessary. There is no need to provide a viable line of access to and from the system unless it's absolutely necessary. A modem could provide just such access.

7.7. Notebook Drives

All notebook drives will be protected through encryption software (Bit-locker) available in the Vista operating system.

7.8. USB Drives:

Hacked USB drives inserted into machines with auto-run enabled and can run malicious code and act as a means of disseminating Trojans and other spyware. USB and for that matter CDs and DVDs must be from reliable sources. Beware of freebie USB drives picked or given as gifts. The USB auto-run OS feature is turned-off on all agency machines via user profiles on all machines unless absolutely necessary to the user.

Special care must also be taken when placing data of any sort, especially confidential data on a USB due to ease by which they can be lost or misplaced. In general, USBs should be avoided as a means of moving any type of sensitive data even if encrypted.

Where possible only certain users will be allowed to copy files onto removable storage devices like USB drives and then only encrypted data.

7.9. Internet Access:

Internet access should be granted to employees only to the extent they need it to perform their jobs. More and more staff are finding useful, job related, services on the internet. However, some job functions do not require unlimited access. At least some filtering will be in force for all.

7.10. Job related sites: Remind all users that the Internet (and all system activity for that matter) is for approved use only: There are countless Internet sites and activities that have no positive influence on the public education environment.

7.11. Acceptable Use and Confidentiality Agreements:

All users are required to sign the USOE's Acceptable Use and Confidentiality agreements before receiving access to the network. Signed and filed agreements (see Appendix I and Appendix M) verify that users have been informed of their responsibilities and understand that they will be held accountable for their actions. Computer services will work with HR to determine appropriate action for violating security policies on a case by case basis. See Appendix Q for guidelines

7.12. Placement of Resources and Firewalls:

All servers, data and information that are intended for direct access by external and in many cases public users must be located outside of the firewall or in a DMZ sub-network. These will generally be static web pages. Dynamic pages which retrieve data from backend databases will make secure calls to those databases which will reside behind firewalls.

7.12.1. The USOE's public Web servers that are intended to provide information and services to the public must be located in such a DMZ. Such Web servers must not be able to access confidential information that resides inside the firewall. This way, if the a public Web server should ever be compromised, confidential information is still protected. All development for such Web servers must take place within a test environment within the network.

7.12.2. After testing, public web pages are published to a staging Web server inside the firewall that continually synchronizes or updates the production Web server outside the firewall. If the public Web server ever fails it can be quickly be rebuilt from this staging Web server.

7.13. Protection of transmissions sent over the Internet:

7.13.1. SSL: Secure Sockets Layer (SSL) enabled servers must be used to secure all private information transactions made with a Web browser: In a secure Web session, the Web browser generates a random encryption key and sends it to the Web site host to be matched with its public encryption key. The browser and the Web site then encrypt and decrypt all transmissions

7.13.2. Digital signatures/certificates: Wherever possible digital signatures are recommended for transmission of sensitive documents over the network via e-mail of other means. By requiring an authentication agent or digital certificate, you force the person on the other end of the transmission to prove his or her identity. In the digital world, trusted third parties can serve as certificate authorities--entities that verify who another user is.

7.13.3. Secure FTP: The USOE has established a secure FTP site where authentication is required and all transmissions to and from the site are encrypted. All files whether or not they contain private or otherwise sensitive information coming into or leaving the USOE network must make use of this site. All files are included. If the USOE provides any place to transfer files that is not secure the chance of data being placed creates a risk.

7.14. Virus Protection

7.14.1. Client antivirus, anti-spyware and firewall software: All devices, clients (desktops, notebooks, PDAs and smart phones) and servers attached to the USOE network must have the agency's prescribed antivirus, anti-spyware and firewall software installed.

7.14.2. Installation: All machines come to the user with the antivirus, anti-spyware and firewall software agents pre-installed by network staff. .

7.14.3. Upgrade/Updates: All updates/upgrades to either the antivirus engine or data files (used to identify virus signatures) are automatically pushed to the individual client machines at logon. The same type of process occurs for anti-spyware and personal firewalls.

7.14.4. Monitoring: All clients are monitored for currency of their antivirus, anti-spyware and firewall software. Sometimes machines are so infrequently attached to the network or the automatic updating is unsuccessful that manual intervention is required.

7.14.5. Communication with vendor: Although the latest data/ID "patches" are automatically pushed to the USOE by the vendor, the USOE network staff also monitors vendor initiated and other virus and spyware alerts.

7.14.6. Response to attacks: In the case of an actual virus or other attack a response plan has been established. See Appendix J.

7.15. Backups – USOE Computer Services has a comprehensive back up system.

7.15.1. Hardware Scope: All servers are backed-up as well as critical operating software for various switches, routers and firewalls. Individual client workstations are not backed up and users are so advised to keep any important data on network servers.

7.15.2. Software scope: All original operating system software, along with service packs and other upgrades are securely backed up and kept offsite. Also all commercially purchased and custom developed software are also backed up and kept offsite. This includes all application software.

7.15.3. Backup hardware and software: USOE uses the latest versions of nationally known and highly rated backup software and the models of popular backup drives. Service and support contracts are in place for all backup software and hardware. In 2007 the USOE began a migration to all disk based backups with eventually placement in a "hot" offsite location. Tape will continue to be used as a final tier.

7.15.4. Data scope: All user "H:" drives and group "G:" drive are backed up. Also, all database software, documents, web pages etc. are backed-up on all servers.

7.15.5. Backup schedule: See Appendix K.

7.15.6. Encryption: Backup software includes an encryption option when backing up sensitive information to ensure that unauthorized users cannot access backup files.

7.15.7. Verification: USOE's backup software allows for verification of backups to ensure they are written to the disk or tape accurately:

7.15.8. Rotation of backup tapes: New tapes are routinely cycled into the tape library and ones that have gone through too many backup cycles are replaced.

7.15.9. Logs: Logs of all backup dates, locations, and responsible personnel are kept on a daily basis. They are very important if and when data of any type needs to be retrieved form offsite storage.

7.15.10. Test of backup system: In the course of normal events the backup system is periodically tested when users ask to retrieve some data that was accidentally deleted. Restorations of full servers should also be tested. More comprehensive restorations exercises are also scheduled.

7.15.11. Off-site location for critical backup copies: Backups of any and all software, databases, and information that serve critical functions reside in a very secure off-site location and are readily accessible when and if needed. Backup data is treated with the same level of confidentiality as production copies. Periodically checks are made to make sure the backups function as expected.

7.15.12. Off-site frequency: Tapes are transported to offsite storage and are picked up on a weekly basis.

7.16. Disaster Recovery/Contingency plans:

In 2002 the USOE developed its first comprehensive contingency and disaster recovery plan. Information Technology was a big part of that plan. The plan is now reviewed and updated twice a year in December and June. The contents of the plan are burned to multiple CD ROMs and distributed to key agency personnel including an associate superintendent, the IT director and the network administrator. Among other items it contains: all emergency contact numbers, hardware inventories; network diagrams; descriptions of how and where all software and data are backed up; formatted descriptions of all USOE systems; circuit lists; and a plan for rebuilding the data center from scratch. See Appendix L. The current disaster and recovery plan would take at least a month, probably more, to execute. Computer Services is in the process of rewriting the entire plan around new backup procedures that eliminate all tape and make us of an off-site backup facility. This does not include temporary employee workspace.

7.17. Inventories:

Inventories of all assets are maintained, including information (data), software, hardware, documentation and supplies. For each server, client workstation and networking device there is included: the manufacturer's name, model, serial number, and other supporting information like operating system, date of install and responsible party.

8. Training.

8.1. USOE acceptable use policies and other important user policies and parts of this security plan must be kept visible throughout the workplace (e.g., banner pages, posters, FYI memos, and e-mail broadcasts).

8.2. Security training in general

8.2.1. Training should be tailored to meet the requirements of the security policy and staffing needs.

8.2.2. Many computer users have never been trained to properly use technology. At most, they many have learned only how to use a particular piece of software or a specific application or two.

8.2.3. The majority may have little understanding of security issues, and there is no reason to expect that to change unless the USOE does its part to correct the situation.

8.2.4. Staff must be adequately prepared for making security policies a part of the work environment.

8.3. Employee Training Outline:

8.3.1. Raise staff awareness of information technology security issues in general.
8.3.2. Include broad overview
  8.3.2.1. What is information security?
  8.3.2.2. Why does it matter?
8.3.3. Data storage
  8.3.3.1. Secure removable storage, destroy confidential paper documents
  8.3.3.2. No removal/extract of sensitive/confidential data from the network servers
  8.3.3.3. No storage of sensitive/confidential data on local or removable storage devices
  8.3.3.4. Scan for sensitive data
  8.3.3.5. No
8.3.4. Security Threats
  8.3.4.1. Social engineering
    8.3.4.1.1. Scams and fraud
    8.3.4.1.2. Phishing
    8.3.4.1.3. Chain letters
    8.3.4.1.4. Hoaxes
  8.3.4.2. Viruses, worms, direct attacks
  8.3.4.3. Vulnerable
  8.3.4.4. E-mail safety
  8.3.4.5. Updating desktop software
  8.3.4.6. Updating laptop software
  8.3.4.7. File sharing
  8.3.4.8. Instant Messaging
8.3.5. Computer use permissions and rights
  8.3.5.1. Regular users
  8.3.5.2. Power users
  8.3.5.3. Administrators
  8.3.5.4. Why risks with higher levels of permissions and rights
8.3.6. Physical access to systems
  8.3.6.1. Servers
  8.3.6.2. Desktops
  8.3.6.3. Laptops
  8.3.6.4. Unattended systems
8.3.7. USOE IT Policies
  8.3.7.1. Confidentiality Agreement and Acceptable Use Policy

    This document will include a reminder that non-confidential or protected data are public information including e-mails and can be requested.

  8.3.7.2. Computer Services Software Use and Service Agreement
  8.3.7.3. Passwords
  8.3.7.4. Network Standards and Connection Policy
  8.3.7.5. Computer Specifications
  8.3.7.6. Software Approval Form
  8.3.7.7. Standard Software Installations/Non-Approved Software
  8.3.7.8. Terminated employees and reassignments
8.3.8. Guest users
8.3.9. Telecommuting and on-the-road access
8.3.10. Computer help and support
  8.3.10.1. Zone administrators
  8.3.10.2. Helpdesk and help tickets
  8.3.10.3. Basic network architecture

8.3.11. Local, state, and federal laws and regulations governing confidentiality and security
8.3.12. Federal laws
8.3.12.1. FERPA overview
8.3.12.2. FERPA relevance and application (examples that relate to audience duties)
8.3.13. Utah GRAMA (Government Records Access and Management Act)
8.3.14. Security as a team effort; roles to play in meeting security goals and objectives.
8.3.15. Specific security responsibilities of some positions.
8.3.16. Inform staff that security activities will be monitored.
8.3.17. Unintentionally destructive acts (e.g., accidental downloading of computer viruses, programming errors, and unwise use of magnetic materials in the office)
8.3.18. Remind staff that breaches in security do carry consequences.
8.3.19. Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).
8.3.20. Immediately Reportable Incidents
8.3.20.1. Child pornography
8.3.20.2. SSN compromises
8.3.20.3. Credit card Compromises
8.3.20.4. Death threats
8.3.20.5. Enticing and engaging a minor
8.3.20.6.
8.3.21. Violations of policy
8.3.21.1. Warnings
8.3.21.2. Corrective action
8.3.21.3. Disciplinary action
8.3.21.4. Terminal
8.3.21.5. Criminal prosecution

8.4. Training schedule:

8.4.1. All new agency employees will receive security training prior to being assigned a network account.
8.4.2. All existing employees will attend a refresher course or workshop at least once every two years.

8.5. Help Desk:

The USOE help desk continually promotes security by being alert for situations that might compromise the safety of the USOE network including all computing and storage devices and is ready with security advice and recommendations to individuals and groups of individuals.

8.6. Reference materials:

Whenever possible Computer Services will develop and distribute or post online reference materials (e.g., checklists, brochures, and summaries).

8.7. Handbook:

The USOE HR rules and employee handbook will be kept up to date online with relevant and current security policies, including the following:

8.7.1. Who approved the policies

8.7.2. Whose authority sustains the policies

8.7.3. Which laws or regulations, if any, on which the policies are based.

8.7.4. Who enforces the policies.

8.7.5. How the policies are enforced.

8.7.6. What information assets are being protected

8.7.7. What users are actually required to do

8.7.8. How security breaches and violations should be reported

8.8. Notification: As part of their security training and posted on the Computer Services and Human Resources Websites employees will be told:

8.8.1. What is and is not acceptable use of technology resources.

8.8.2. Computer services will work with HR to determine appropriate action for violating security policies on a case by case basis. See Appendix Q for guidelines

8.8.3. That their activities may be monitored.

8.8.4. That agency computers are not for personal use and must not be misused

8.8.5. There should be no expectation of privacy for personal employee information stored on or transmitted within the USOE's technology infrastructure. This will pertain mostly to e-mail

8.9. Acceptable Use and Confidential Policies Acknowledgements.

Employees are required to sign the agency acceptable use and confidentiality agreements that include security provisions (see Appendix I and Appendix M) to acknowledge that they are aware of their responsibilities and verify that they will comply with these policies. This requires that:

8.9.1. Staff should have ample opportunity to read and review all policies and regulations for which they will be held accountable.

8.9.2. Staff should be provided an appropriate forum for clarifying questions or concerns they may have about the organization's expectations.

8.9.3. Staff should not be given access to the system until signed agreements are accounted for and maintained in a safe place.

8.9.4. All new employees should be expected to meet the organization's security requirements and procedures as a part of their job description. Once hired, new employees should be informed of, and trained on, acceptable use and security policies as a part of their initial orientation in order to impress the importance of security upon them.

8.10. Security Training Outline

8.10.1. Raise staff awareness of information technology security issues in general.

8.10.2. Include broad overview

8.10.2.1. What is information security?
8.10.2.2. Why does it matter?

8.10.3. Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security

8.10.4. Stress Federal laws

8.10.4.1. FERPA overview
8.10.4.2. FERPA relevance and application (include specific examples that relate to audience duties)

8.10.5. Stress state laws, regulations, and standards including GRAMA (Government Records Access and Management Act)

8.10.6. Explain organizational security policies and procedures.

8.10.7. Ensure that all employees understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.

8.10.8. Train staff to meet the specific security responsibilities of their positions.

8.10.9. Inform staff that security activities will be monitored.

8.10.10. Remind staff that breaches in security carry consequences.

8.10.11. Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).

8.10.12. Stress that unintentionally destructive acts (e.g., accidental downloading of computer viruses, programming errors, and unwise use of magnetic materials in the office) are the source of many security risks.

8.10.13. Review results of risk assessment findings along three broad areas that include: assets, threats and vulnerabilities.

8.10.14. Review USOE security policies, procedures, and regulations within the main areas and focus on those related to audience's duties.

8.10.14.1. Physical security regulations

8.10.14.2. Information security regulations

8.10.14.3. Software security regulations

8.10.14.4. User access security regulations

8.10.14.5. Network security regulations

For online version, where possible Replace with links to files in appropriate directories in: \\beweb\inetpub\public\computerservices\policies...

Appendix A:

PRIVACY AND USOE DATA

FERPA

1. ***Purpose:*** The federal Family Education Rights and Privacy Act assures parents access to their students' education records and protects the parents' and students' right to privacy by limiting the availability of student records without parental consent.

2. ***Rights established by FERPA:*** There are three general rights: (1) the right to inspect and review education records relating to the student and maintained by the school the child attends or has attended; (2) the right to challenge and require the school to amend a record concerning the student that is inaccurate, misleading or otherwise in violation of the student's privacy rights; (3) the right to require the school to obtain written consent prior to the disclosure of personally identifiable information, subject to specific exceptions.

3. ***"Education records":*** Usually defined as "…those records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational agency or institution …" regardless of the format the record is in. The definition includes personally identifiable information about students collected and maintained by USOE. This would include student test answers, it does not include the actual tests.

4. ***Parental Consent NOT required:*** USOE does not need to have parental consent to provide data:
   a. ***That is not personally identifiable—***aggregate test scores, for example.
   b. ***To school officials, including teachers, who USOE determines have a legitimate educational interest in the student.*** This might include disclosing the information to the student's teacher, but might not include disclosing it to someone the teacher says should see it.
   c. ***To officials of another school, school system or postsecondary institution where the student seeks or intends to enroll.***
   d. ***To the comptroller general of the United States or the Secretary of Education of state and local educational authorities*** *in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or in compliance with requirements related to those programs.*
   e. ***To an organization conducting studies on behalf of USOE*** *to (A) develop, administer or evaluate predictive tests; (B) administer student aid programs; or (C) improve instruction.*
   f. ***To accrediting organizations*** *to carry out their accrediting functions.*
   g. ***To the parents of the student,*** *custodial or non-custodial.*
   h. ***To comply with a judicial order or subpoena****, though the agency must make a reasonable effort to notify the parents about the subpoena before complying with it.*
   i. ***In connection with a health or safety emergency****.*

5. ***When disclosures are made:***
   a. USOE must create a log whenever it provides personally identifiable information to someone other than the parents. The log should include: (1) the parties who have

requested or received the education records; and (2) the legitimate interest the parties had in requesting and obtaining the records. The log should also include the date the request was received and the date records were actually provided.

b. USOE may charge for the reasonable costs of producing records and need not provide the records in any particular format.
c. If a parent requests a record, USOE has 45 days to make the record available. FERPA gives parents the right to "inspect" the record, which does not include having copies sent to them. The only time FERPA requires copies is if refusing to copy the record would effectively deny the parent access to the record, i.e. if the parent lives in another state.

6. ***What records does USOE maintain that would be subject to FERPA?***

d. Test scores attributable to an identifiable individual. Parents have a right under FERPA to see the results of their student's tests. Parents **do not** have a right to see the actual state tests.
e. Aggregate data that identifies the student because the numbers are so small. For example, an aggregate of the ethnic students who dropout of a particular school or even a district may include so few Asian students that the students become identifiable because there are only two Asian students in the district. Data that does identify students in this matter must be used in compliance with FERPA.
f. Student enrollment data. USOE is **not** a general source of information regarding the location of students. Persons seeking to know where a student is enrolled must be the parent of the student and/or have court documentation requiring USOE to release the data, per FERPA

7. **Additional FERPA Information**

FERPA which became law in 1974 has been amended 29 times to date (20 U.S.C. § 1232g; 34 CFR Part 99). In protecting the privacy of student education records the law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education FERPA Fundamentals. See: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students.

i. Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

ii. Schools must have written permission from the parent or eligible student in order to release any information from a student's education record except for those cases listed in part 4 above

iii. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible

students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

b. FERPA and USOE. The USOE collects large and detailed amounts of data from schools each year including data about individual students within the Utah public education system. The identity of a student is masked as much as possible. No names are associated and linking identifiers or keys have been encrypted to prevent such linking and identification of individual students from the district accessible portion of the Statewide Student Identifier (SSID) system.

GRAMA—Government Records Access and Management Act

1. Teacher records: CACTUS records are not protected by FERPA. Anyone can request access to CACTUS data, but GRAMA only requires USOE to provide certain specified information about employees: work phone numbers and addresses, gross compensation, job descriptions and the teacher's qualifications for the job, such as college degrees earned.
2. USOE must respond to a GRAMA request within 10 days of receiving it. The response may be "no, and here's why (the information doesn't exist, you aren't entitled to receive it, etc)," "Yes, and here you go," "yes to the attached items and no to the rest of your request," or "yes, but we need x number of days or weeks to compile the data." GRAMA requests for anything other than data that is clearly public record should be forwarded to USOE Legal for review.

Appendix B

USOE Power User's Guide

September, 2005

Definitions:

Standard User: Most USOE users fall into this category. These users have full access to USOE services and where appropriate, they have permission to write to certain directories on certain servers. The services include among others: e-mail, customer applications, Internet browsing, desktop productivity tools (word processing, spreadsheets, etc.), as well as the ability to store data on local storage devices and sync handheld devices. What a standard user cannot do is alter the basic configuration of or install software on agency computers.

Power User: The power user has more control of the local machine than the standard user. While the standard user can save data on the local machine and change certain properties such as desktop themes, the power user can install software after receiving permission from the network administration staff. The software the power user can install may include new versions or enhancements to the basic operating system or other system software such as PDA synchronization devices. In the case of a power user who is also a USOE zone administrator, they will also be able to perform those same services for standard users within their zone.

The number of users designated as power users or administrators should me minimized as much as possible. Yearly reviews of all power and administrative users must be conducted to determine if they are still eligible for such designations. A similar review should take place when a power user or administrator changes positions.

Qualifying to be a Power User:

- **Network Professionals:** By definition, administrative users, who are almost always professional network specialists and are very limited in number, are also power users.
- **Zone Administrators and Automated System Support Specialists:** By nature of their special assignments, in sections where such individuals have been designated, they are power users. In some cases, due to the duties specific to their assignments they may have even more rights and permissions than the typical power user. Examples include someone who needs to grant security permissions to users on a server or install software on other users' machines.
- **Developers/Programmers/Web Masters:** Anyone who develops custom software may have a need to have greater access to their local machine resources than a standard user. Such positions frequently require the installation and removal of various types of software that include but are not limited: to software development software, database systems, and software management tools.

- **Other Users Who May Qualify as Power Users:** Although requests for the status of power user will ultimately have to be considered on a case-by-case basis by the professional network staff and require the sign-off of the requesting user's supervisor, the following is a representative list of those who may qualify. Ultimately, qualification depends on the scope and frequency of activities such as those described herein.

    - Curriculum specialists who frequently need to evaluate various computer based instructional packages from commercial and other sources

    - Media specialists who often need to install software used in the production of media or various computer based instructional packages from commercial and other sources

    - Statisticians who frequently need to install and/or upgrade software required to do various types of statistical analyses

    - Others who can demonstrate power user needs similar to those described herein

Procedures:

- The prospective power user can be identified either by himself or herself, a supervisor, or the network staff.

- The prospective power user is required to submit a written request to the USOE IT Manager explaining why power user status should be granted. This request must be signed by his or her supervisor or forwarded via e-mail from his or her supervisor.

- The IT Manager along with network administration staff will review this request and notify the applicant and supervisor whether or not they agree with the request. If the request is agreed upon, the applicant will be required to complete the USOE Power User Agreement Form.

- While functioning as a power user, the user is still required to follow the Agency's and the State's Acceptable Use Policy.

- The power user must obtain permission from specified network staff what software they are planning to install before doing so by completing the USOE Software Approval Form. Network staff will review and respond to these requests as top priority items. Special arrangements may have to be made in some cases to cover emergency situations.

- The power user must be especially vigilant to ensure against installing any unlicensed software.

- In the event the power user has technical problems with his or her machine as a result of some installation or modification they perform, and need assistance, they will need to submit the usual help desk request. Their status as power users does not imply priority service from the network staff.

- If the power user encounters repeated problems requiring network staff intervention or is in violation of the USOE Power User Agreement, their power user status will be revoked until further review.

Appendix C

USOE Power User and Local Administrator Agreement

April, 2006

I _____ have requested
(Please Print Your Name)

☐ Power User, or

☐ Local Administrator privileges

on the following machine: _____, and
(Please print machine name)

agree to the following:

1. I attended the USOE Power User and Local Administrator Security Training on _____.
(Date)

2. I will not add, remove, or disable ***any software*** on the above machine without IT permission. (See the USOE Software Approval Form to request permission).

3. I will not add, remove, or modify any local administrator accounts without IT permission.

4. In the event that any software fails to function properly on the above listed machine due to my not following this agreement, I will assume full responsibility. Should I require IT assistance, I will submit a help box ticket and understand that IT assistance will be provided as time permits.

5. I understand that violation of my power user/administrator privileges will result in my privileges being revoked until further review.

Employee Signature: _____

Date: _____

Division Director: _____

Date: _____

Appendix E

Currently under revision to employ more agile/SCRUM methods – scheduled to complete by 10-1-07

Software Development Life Cycles: Outline for Developing a Traceability Matrix

By Diana Baldwin, AccuReg Inc.

1. Software Life Cycle
    1. The FDA does not prescribe a specific software development life cycle, but requires manufacturers to identify and follow what makes sense for them
    2. Manufacturers choose a software life cycle model and development methodology appropriate for their device and organization
        1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998
    3. Software Life Cycle must include:
        1. Risk management
        2. Requirements analysis and specification
        3. Design (both top level and detailed)
        4. Implementation (coding)
        5. Integration
        6. Validation
        7. Maintenance
    4. A software life cycle model should be understandable, thoroughly documented, results oriented, auditable, and traceable.
        1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998

2. What is required to demonstrate traceability?
    1. Provide a traceability analysis or matrix which links requirements, design specifications, hazards, and validation. Traceability among these activities and documents is essential. This document acts as a map, providing the links necessary for determining where information is located.
        1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998

3. How Does Traceability Ensure the Life Cycle is Followed?
    1. It demonstrates the relationship between design inputs and design outputs
    2. It ensures that design is based on predecessor, established requirements
    3. It helps ensure that design specifications are appropriately verified, that functional requirements are appropriately validated
    4. Important: Traceability is a 2-way street. Maintain "backwards" and "forwards" -- Tunnel Vision not acceptable in the Software Life Cycle!

4. Traceability Across the Life Cycle
    1. Risk Analysis (Initial and Ongoing Activities)
        1. Trace potential hazards to their specific cause
        2. Trace identified mitigations to the potential hazards
        3. Trace specific causes of software-related hazards to their location in the software
    2. Requirements Analysis and Specification
        1. Trace Software Requirements to System Requirements
        2. Trace Software Requirements to hardware, user, operator and software interface requirements
        3. Trace Software Requirements to Risk Analysis mitigations
    3. Design Analysis and Specification
        1. Trace High-Level Design Specifications to Software Requirements
        2. Trace Design Interfaces to hardware, user, operator and software interface requirements

3. Evaluate design for introduction of hazards; trace to Hazard Analysis as appropriate
4. Design Analysis and Specification
    1. Trace Detailed Design Specifications to High-Level Design
    2. IMPORTANT: Ability to demonstrate traceability of safety critical software functions and safety critical software controls to the detailed design specifications
5. Source Code Analysis (Implementation)
    1. Trace Source Code to Detailed Design Specifications
    2. Trace unit tests to Source Code and to Design Specifications
        1. Verify an appropriate relationship between the Source Code and Design Specifications being challenged
6. Source Code Analysis (Implementation)
    1. Trace Source Code to Design Specifications
    2. Trace unit tests to Source Code and to Design Specifications
        1. Verify an appropriate relationship between the Source Code and Design Specifications being challenged
7. Integration
    1. Trace integration tests to High-Level Design Specifications
    2. IMPORTANT: Use High-Level Design Specifications to establish a rational approach to integration, to determine regression testing when changes are made
8. Validation
    1. Trace system tests to Software Requirement Specifications
    2. Use a variety of test types
        1. Design test cases to address concerns such as robustness, stress, security, recovery, usability, etc.
    3. Use traceability to assure that the necessary level of coverage is achieved

5. Plan Ahead for Traceability
    1. Options
        1. Manual methods
            1. Word processors
            2. Spreadsheets
        2. "Home-built" Automated Systems
            1. Relational Databases
        3. Commercial Automated Systems
            1. DOORS
            2. Requisite Pro

Appendix F

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

Section 1: Change Request Information

To be completed by Requester except shaded areas, see DETAILED INSTRUCTIONS BELOW. All requests should be e-mailed by a Director/Coordinator or Associate Superintendent to dwhite@usoe.k12.ut.us

Originator (Title)		**CR Type:**	☐ **Change to Existing System or Project** ☐ **New System or project** ☐ **Other Temporary or One-Time Project**
Director/Coordinator			
System Name	**CRT**		
Or… Project Name	**Science Tests Extract**	**CR No:**	
Or… Other		**CR Log Date:**	
		CR Resolved Date:	
Desired Date			

1A – Description of Change Being Requested: (Describe the requested change. Provide attachments if additional explanation is needed.)

1B - Proposed Solution (optional): (Provide your opinion regarding the best course of action, based on factors such as cost, schedule, or product quality. Provide attachments if additional explanation is needed.)

1C - Risk Impact: (Provide your opinion regarding the risk of not doing the change, based on factors such as cost, schedule, or product quality. Provide attachments if additional explanation is needed

1D – Quality Assurance/Controls: (Describe how you plan to help provide for quality of the data/information involved

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

in the system/project. What controls will be implemented and who will be responsible to work with Computer Services to ensure such quality and controls. Provide attachments if additional explanation is needed.)

Section 2: Priority Assessment (Use Service Level Agreements in Change Management Process Document)

Service Level Agreement Used: ☐ **Applications** ☐ **Project** ☐ **Other**

Assigned Service Level: ☐ **(1)** ☐ **(2)** ☐ **(3)** ☐ **(4)** ☐ **(5)** ☐ **New Project Required**

2A – Justification for Priority

Section 3: Impact Analysis (To be completed by Computer Services or Project Management)

3A - List Artifacts Affected

5B- Overall Impact:

Business Assessment: (Briefly describe the anticipated benefits, and document any changes to the workflow/operational procedures which might result from this change.)

Completed by: *Date:*

Technical Assessment: (Briefly describe how existing services or deliverables will be affected as a result of the requested change. Describe acceptance criteria for changed deliverables. Attach documentation such as the functional

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

	specification to illustrate, as needed.)
Completed by:	*Date:*
Cost Assessment:	(Briefly describe changes to the Resource Plan that would result from this change.
Time Assessment:	(Briefly describe changes to the Project Schedule that would result from this change. Attach copies of existing and new schedules showing new tasks, subtasks, and milestones.)
Completed by:	*Date:*

3C- Potential Risks:		
3D – Management Approval:	**Phone:**	**Date:**

Section 4: Disposition of CCB (To be completed by Computer Services or Project Management)

Disposition Assigned:	☐ Pre-Approved	☐ Approve	☐ Deny	☐ Defer	☐ More Info
Assigned Service Level:	☐ **1 (Pre-Approved)**	☐ **2**	☐ **3**	☐ **4**	☐ **5** ☐ **New Project Required**

Changes which are not approved within ten (10) work days will be considered to be rejected.

4A – Recommendations and Communication Plan/:

4B – Action Items

Action Item	Due Date	Responsible	Status

4C - CCB Approval: (Project Management Office)	**CCB Date:**

Section 5 - Closure	**Completed**	**Date Completed**
• Communication to impacted parties	☐	
• Artifacts updated	☐	
• Project Plan updated	☐	

Instructions

- Orignator fills in Section 1 *(excluding the CR number assignment, Logged Date and Resolved Date)*
  - *Specify if CR is for an existing system (including IT infrastructure) OR existing project OR other*
  - *If CR is for an existing system or project, specify the parts of the system/application needing change. Provide details in section 1. See examples below.*
  - *If CR is for a project, specify the deliverable where the change would occur.*
- PMO assigns the next available Change Request Number
- Project Management completes Section 2
- CCB completes Section 3
- Project Management completes Section 4

Section 1 (General information)	
• Provide unique description • Enter Priority Rating • Enter date needed by	***Examples: Forms, Reports, Data Field, Labels, Color, Business Rules, Error messages, Desired services, Desktop environment, etc.***
Section 1A (Requester's Description of Change)	
• Explain why the change is required • Provide a narrative of any problem	***Provide business or technical justification. Provide a step by step description of any problem so that it can be reproduced by the computer services staff.***
Section 1B (Proposed Solution) • Provide a brief description of proposed solution	
Section 1C (Risk Impact) • Provide a brief description of risk if change is not made	**Describe the consequence of not implementing the CR. Describe consequences of implementing the CR**
Section 2A (Impact Analysis)	**Identify who performed the assessment in each sub-section.**
• List Artifacts affected and their owners	**List all artifacts requiring work if the change is implemented. Use *Impact Analysis For.* Place summary of impact in this section. List all new, modified or deleted artifacts**
Section 2B (Overall Impact) • Explain how each artifact or function is affected • List all processes and functions affected	**Describe the following criteria:** • **Work: Expected number of hours to complete the change** • **Resources: The types of resources needed and their availability. Describe conflicts with other work assignments** • **Schedule: Estimate the amount of time in calendar weeks to implement the change. For projects, calendar days should be used.** •
Section 2C (Potential Risk) • Identify potential risk(s) • Obtain Project Manager's approval	

Section 2D (Track Lead Approval)

- Director of Computer Services must approve all CR's in order to be submitted to CCB for disposition

Section 3 (Priority Assessment)

- Service Level Agreement Used
- Priority Assigned
- Justification for Priority

Section 3 (Disposition of CCB)

- Status
- Recommendation
- Action Items
- CCB Approval

Section 4 (Closure)

- Notify affected entities
- Artifacts updated
- Project Plan updated

Appendix H

USOE Network Standards and Connection Policy
(Definitions of *bold & italicized* **terms are listed at the bottom.)**

Two classes of computers may connect to the *USOE network***. Please note the restrictions that apply to each class.**

1. Owned by the USOE.

This computer may be connected directly to the ***USOE domain*** via cable.

All USOE owned machines are purchased, installed, configured, and maintained according to ***USOE hardware and software standards*** by network administrators.

Additional software may be installed only with the approval of the USOE network administrators. If the USOE owned computer is a notebook, it may also be used for ***telecommuting.*** It may be configured for ***VPN*** to access the ***USOE domain*** from the Internet or through the ***USOE wireless network segment***.

Only USOE owned computers will be allowed to connect to the USOE domain, directly or indirectly through a VPN connection.

2. Privately owned and brought into the USOE by a business visitor.

A business visitor may access the Internet, but not the ***USOE domain***. USOE has an open wireless system that visitors can connect to. To access the Wireless Internet, they must receive permission along with the current username, password, and instructions from a USOE employee in order to connect to the ***USOE wireless network segment***. With these credentials, the business visitor is responsible for configuring, and establishing the wireless Internet connection. If the business visitor does not have a wireless network adapter, they may still connect to the Internet via cable and specially marked data jacks in conference rooms throughout the building.

The business visitor must be asked to assure their host they are using a ***secure computer*** and are willing to abide by the ***Acceptable Use Policy***.

Note about PDAs (personal digital assistants). No PDA or other handheld device may, by itself, be directly connected to the USOE network, wirelessly or with cable. When properly configured such devices may be used to synchronize with the host computer or download network files including those in Outlook, This is only permissible through a USOE owned or ***telecommuting*** computer by means of an attached cradle or Bluetooth wireless technology. **Violators of this policy may be subject to disciplinary action.**

USOE is not responsible for lost data or damage to any privately owned machine that is connected to *USOE wireless network segment* or the *USOE domain*.

Definitions

Acceptable Use Policy. All employees and business visitors, regardless of how they are connected to the USOE network are required to follow the USOE acceptable use policy. See: http://www.usoe.k12.ut.us/hrm/acceptuse.htm & http://www.governor.utah.gov/lan/aup.htm. Also note the acceptable use policy states:

Also, please note the acceptable use policy states that the use of resources for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc., or other uses that waste resources or disrupts performance, is prohibited.

This includes use of agency machines for streaming audio and video when not work-related. **Violations of the acceptable use policy may be grounds for termination.**

Telecommuting. USOE employees may telecommute with management approval. Telecommuters must use a USOE owned computer. If the telecommuter desires to connect to the ***USOE domain*** through the Internet and ***VPN***, they must secure their own Internet connection. See http://www.usoe.k12.ut.us/hrm/rules2002.pdf for more information about telecommuting.

USOE domain. The USOE domain is the secure network of shared computers at the USOE. It is a subset of the more generally defined ***USOE network***. The domain includes all servers and user computers, each connected to one or more of those servers. These machines are all behind a firewall and other security devices and software such as intrusion detection and filtering servers. When a user connects to the USOE domain from within the building by supplying a logon name and password they also receive Internet access. Business visitors are permitted to connect to the USOE wiring infrastructure and obtain Internet access without connecting to the USOE domain. Such use is permitted only through the ***USOE wireless network segment***.

USOE hardware and software standards. In order to maximize usability, reliability, security, and efficiency of USOE information technology resources; the USOE has defined hardware and software standards. A summary of the current hardware/software standards include: a Dell desktop or notebook running Windows XP with the latest service packs and updates installed, and the latest Microsoft Office suite of productivity applications including the Outlook e-mail client. As part of the USOE standard setup features, these machines are all configured as ***secured computers***. Other hardware and software standards exist in the USOE, but most involve network infrastructure and custom application development and deployments. Always check with network administrators before purchasing software or hardware to see if it is compatible with the USOE network, and if an agency license agreement (in the case of software) already exists. Installation of software for purely personal use is prohibited. All installed software must be for work related activities and must be owned by USOE.

USOE network. The USOE network is defined as the entire computer infrastructure within the USOE including all wiring, communication devices, routers, switches, servers, desktops and other connected computers. The ***USOE domain*** is a subset of this network.

USOE wireless network Segment. A secure wireless network segment is available for USOE staff and sponsored business visitors. This network provides access to the Internet and optionally to the USOE domain via VPN. In order to connect to the USOE for Internet and/or USOE domain access, the

USOE employee or business visitor must first acquire the current credentials and configure the computer to recognize and connect to the USOE wireless network segment. For security reasons these credentials may change periodically. When this happens they will be distributed to all USOE employees who have a VPN account. Currently the USOE supports the IEEE 801.11b and 801.11g wireless protocols.

VPN (virtual private network). VPN allows those with USOE domain accounts to access the USOE network remotely or through the firewall. You must have a VPN account established by a USOE network administrator before you can access the domain using VPN. Only network administrators will be able to configure VPN access. If you need VPN access please contact the Help Desk.

Appendix I

Confidentiality Agreement

As an employee of the Utah State Office of Education (USOE), I acknowledge that in the course of my employment I may have access to confidential data and information. This policy provides protection for USOE employees as well as notice of inappropriate and unprofessional behavior.

At all times during and after my employment by the USOE, I agree to follow the directives of the USOE Security Plan (see: http://www.schools.utah.gov/computerservices/Policies/USOE Security Plan1.doc). In any instance in which the terms of this agreement are more restrictive than the USOE Security Plan, the terms of this agreement shall govern.

I acknowledge that in the course of my employment as a Utah State Office of Education employee I may have access to data in print or electronic form that contains confidential individual data.

I understand that, I may be disciplined and/or dismissed from employment if found to be in violation of this Agreement or the USOE Acceptable Use Policy below; and that, under state and federal law, misuse or mishandling of data acquired and maintained by a public agency or that agency's information technology may result in criminal and/or civil action against the employee.

I understand and agree that:

- **Confidential Information includes, without limitation, any individually identifiable student, teacher, client, employee or customer data, including all data that are protected by the Family Educational Rights and Privacy Act (FERPA). FERPA provides for the protection of student information by setting forth principles for the gathering and handling of student level data.**

  Confidential information also includes confidential or secret information necessary for the proper functioning of the public education system. Such information includes high-stakes test questions and keys, as well as professional practices cases.

- **The Internet provides the ability to communicate, collaborate with others and access information anywhere. Within the USOE network email files are protected from outside access. However, anything transmitted over the Internet is subject to interception, reading, and copying by others. Do not transmit personal information about yourself or anyone else using USOE resources without proper authorization. The confidentiality of such material cannot be guaranteed. Use caution when sending confidential information.**

  The USOE has the right to access and disclose the contents of electronic files, as required for legal, audit, or legitimate state operations management purposes (Administrative Rule R365-4). Email and other electronic files may be accessible through the discovery process in the event of litigation. Each of these technologies may create a record and therefore are reproducible and subject to judicial use.

- I will access and distribute confidential data and information only as needed to conduct USOE business and within the scope of my specific assignment(s); and will not store confidential

information on any computing or storage media not owned by the USOE. Even when owned by the USOE such media must be secure. These do not include desktop or notebook computers.

- I will not store work related data on local machines except for incidental and temporary use. Personal or other sensitive data must never be stored on a local machine or peripheral device.

- I will maintain the confidentiality of all such data and will not disclose (whether verbally, electronically, by document or any other form of communication) any such information to any person except to authorized Agency employees or as authorized in writing by my USOE supervisor.

- I will maintain the confidentiality of my security authorizations (user IDs, passwords, electronic keys, smartcards etc.) and be personally accountable for all work performed under my security authorizations.

- I will protect confidential information displayed on my workstation from inadvertent exposure to passersby.
.
- I will immediately report any security and/or privacy breaches to the Information Technology Director, Network Administration, or USOE network help desk. If I receive or obtain information to which I am not entitled I will also notify one of the above as well as the owner and sender of such information. I will also report any inappropriate use of USOE-provided IT resources.

- Any request for access to information concerning any USOE data by any person other than authorized USOE employees will be directed to the office that owns the data or information.

- I will retain or dispose of electronic records in accordance with the Government Records Access and Management Act (GRAMA). Refer to GRAMA or seek counsel from the USOE records manager for guidance in this area.

- **Section 63-2-801 of the Government Records Access and Management Act provides: A public employee or other person who has lawful access to any private controlled, or protected record under this chapter, and who intentionally discloses or provides a copy of a private, controlled or protected record to any person knowing that such disclosure is prohibited, is guilty of a class B misdemeanor. Furthermore, Subsection (2)(a) of Section 63-2-801 provides penalties against any person who by false pretenses, bribery, or theft gains access to or obtains a copy of any private, controlled or protected record to which he is not legally entitled, and classifies such acts as class B misdemeanors.**

I will not:

- Gain or attempt to gain unauthorized access to USOE data and information.

- Share my user ID(s) and passwords(s) or electronic keys or smart cards with anyone.

- Leave my workstation unattended or unsecured while logged in to USOE data systems.

- Personally use or knowingly allow other persons to use any USOE database or other USOE sources of data for personal gain or other unauthorized use.

- Make unauthorized copies of USOE data or computer applications.

- Negligently or intentionally engage in any activity that could compromise the security or stability of any USOE data system.

Acceptable Use Policy

The USOE characterizes as unacceptable and just cause for termination of use privileges, disciplinary action, and/or legal action, any of the following uses of information technology resources--e.g., computers, copiers, e-mail, fax, Internet, printed material, printers, telephones, video--provided by the agency:

1**. Illegal Use.** Any use for or in support of activities that violate local, state, or federal laws.

2. Infringement of Intellectual Property Rights. Any use in violation of software license agreements or other contractual arrangements relating to the use of copyrighted materials. At all times adhere to all copyright law regarding the use of software, information and attributions of authorship. Upon the request of the agency, delete (from any computer) and return all state-provided software used for off-site work.

3. Commercial Use. Any use for commercial purposes or activities resulting in personal financial gain, including product advertisements.

4. Personal Use. Any use for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc. Documents, photos, and other files of a personal nature are not to be stored on USOE servers.

If you are unclear about the acceptable "personal" use of a state-provided resources or wish to use the resource for what may be considered a good cause, please seek authorization from the USOE network administration through the USOE help desk.

Installing or using instant messaging software other than USOE prescribed software is prohibited. Attaching executable programs to email is also prohibited. It is suggested that only the following file types be attached to USOE email. Never include confidential data in an email or attachment.

- Word processing documents (.doc, .pdf, .wpd)
- Spreadsheet files (.xls, .wb3)
- Presentation files (.ppt, .shw)

5. Offensive or Harassing Material. Any use of material which may be deemed vulgar, sexually explicit or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, or political or religious beliefs.

6. Religious or Political Lobbying. Any use for religious or political lobbying.

7. Security Violations. Any action which threatens the security of agency resources, including but not limited to such actions as: giving your password to another person; accessing accounts for which you are not authorized; or spreading computer: viruses, spyware or other malicious software.

8. Confidential Information. Transmitting information classified as other than "public" under the Government Records Access and Management Act without proper security; or violating the privacy of others by reading e-mail or other private communications (unless you are specifically authorized to support communication systems).

9. Unnecessary Use. Otherwise appropriate use which intentionally wastes resources or disrupts performance by excessively consuming operating time, storage, paper, etc.

10. Use of non-agency owned computing devices on USOE's network. Employees are not permitted to connect non-agency computers (including PDA, phones, etc.) to the USOE network, either through a direct connection, over the internet or over a local wireless segment utilizing a VPN connection. Visitors to the USOE may connect to the Internet through an external wireless segment or through specially marked data jacks in conference rooms. Special arrangements can be made for persons doing work under contract for the USOE.

USOE employees are also bound by the provisions of the Utah Education Network Public Education Acceptable Use Policy. (http://www.uen.org/policy/aup.shtml)

As a general "rule of thumb": Don't say, do, view or acquire anything you wouldn't be proud of having everyone in the world learn about if the electronic records were made public.

Employee Acknowledgement and Acceptance

I have read and understand the USOE Confidentiality Agreement and Acceptable Use Polity and agree with the Confidentiality Agreement and will follow the Acceptable Use Policy.

Name: _____

Wk Phone: _____ Employee ID: _____

Department/Unit: _____ Position: _____

Signature: _____ Date: _____

Supervisor: _____

Supervisor Signature: _____Date:_____

Change history:

April 24, 2006: Added to first AUP bullet: "and will not store confidential information on any computing or storage media not owned by the USOE. Even when owned by the USOE such media must be secure. These do not included

Appendix J

USOE COMPUTER VIRUS RESPONSE PLAN

USOE Anti-virus Environment

E-mail Servers - All incoming e-mail and attachments are scanned and cleaned, if necessary, by the Barracuda SPAM and anti-virus Firewall before going to the e-mail server. Barracuda signature files are updated on a daily basis. If an e-mail message or attachment is found to have a virus it is deleted, logged and replaced with a message notifying the user that this has occurred.

Servers - All servers, including e-mail servers, have the McAfee Virus Scan product installed to check on a daily basis for updated DATS (signature files). It is also checks on a biweekly basis for any upgrades of the anti-virus scanning engine. This product checks all files coming into the server for viruses.

Clients - All client Machines have the McAfee Virus Scan product installed in such a way that it checks on a daily basis for updated DATS (signature files). It is also checks on a biweekly basis for any upgrades of the anti-virus scanning engine. This product checks all files coming into the computer for viruses.

Virus Outbreak Procedure

Virus attacks are an ongoing occurrence. Every day hundreds or thousands of infected e-mails arrive at the e-mail server. Over 99% of these are successfully intercepted by the Barracuda SPAM Firewall (deleted and logged) and cause no damage. A virus can also be introduced from downloads or file copies from other magnetic media. In these cases, the vast majority are detected and deleted by the McAfee anti-virus software. However, on occasion, a machine or machines can get infected. The following is a procedure to be followed in these events. Note, that not every instance of an infection warrants network-wide response. Often the problem can be isolated an dealt with on one machine.

- As a regular preemptive step, the Barracuda Firewall administrator should regularly check the log generated by the Barracuda system to determine if the USOE network is being hit by a heavier that normal number of e-mails or virus contained in messages or attachments. Although the log indicates when viruses have be intercepted and "cleaned", either event may be cause to be on the lookout for other incidents.

- As soon as a reported problem (usually via the help desk) on a client machine or desktop looks as if it is a possible virus, the machine should be disconnected from the network, until the machine can be fully scanned by the most current anti-virus software and it can be determined that it is free from any new undocumented virus.

- If a virus is identified, the anti-virus software web sites should be searched to determine the behavior or the new virus. If no virus is found, but an apparent infection has taken place, an attempt should be made to match the symptoms with those of newly reported viruses in an

attempt to identify the cause of the infection. Again, the anti-virus software vendor web sites should be employed.

- Once the virus has be researched and identified. The directives from the web sites should be followed to mitigate the impact on the internal and external networks.

- If the virus is high risk or widespread, consideration should be made for either shutting down the e-mail server, disconnecting the internal USOE network from the external (Internet) network or both. This decision should be made by the coordinator and communicated from the help desk by e-mail (if possible) to all users, or by phone if e-mail is not operable. In part, this decision may be made based on the volume of e-mail leaving the e-mail server for internal, or more importantly, external destinations. A rapidly increasing volume of e-mail may indicate the virus is being proliferated by the USOE's e-mail server.

- The decision to disconnect the network may also need to be made if the network or parts of the network are under attack from a hacker of some type. Such attacks will more than likely affect only isolated machines (clients or servers), but the potential exists for having to isolate the entire network.

- After all affected machine or mailboxes have been identified and the virus has been contained and cleaned, there may be the need to recovery corrupted data from backup servers or tapes. If the damage is widespread, ad hoc priorities by have to be defined and communicated concerning whose files and/or mail will be restored first.

- Finally, the incident should be described and logged, with recommendations for future prevention.

Appendix K

USOE Back-up Procedures

Definitions: Full: A full backup is a complete back up of all files and the archive bit is reset. **Incremental:** An incremental backup will backup all files that have changed since the previous full or incremental backup.

Backup Overview: We are currently backing up 38 USOE Agency Servers. All data on each server is backed up excluding the Windows directory and the swap file on each server. We have a Dell PowerEdge 1850 Server, Server 2003, Service Tag: G78TH71, with Symantec's Backup Exec Software. We currently utilize a D2D2T (Disk to Disk to Tape) solution. We have a 4TB Fiber attached SAN that the data is written to first, and then duplicate jobs are run which puts the data on tape. The tape drive is a Dell Power Vault 132T, two drives, Service Tag: DM6G921 and utilizes LTO2 tapes. Backup tapes are created, labeled, boxed, picked up and taken to Perpetual Storage every Tuesday morning. A contract with Perpetual Storage, Inc. has been executed. Telephone number: (801) 942-1950. This facility is a fully finished, multi-mezzanine storage area located in a granite vault. It is a guarded facility to which only Perpetual Storage personnel are allowed. The tapes are stored for three years at the facility. After the three year retention date is met, the box is returned to USOE. We may erase the tapes and reuse if possible. If the tapes are not reusable, they are erased and discarded.

Schedule: Full backups are run the first weekend of each month starting Friday at 6:00 p.m. This may be moved to a different weekend depending on maintenance, etc.
Exception: A full backup is run every Friday night on the email server. **Incremental** backups are run nightly, Monday – Friday, starting at 10:00 p.m. The Friday night incremental backups are excluded the weekend of the full backups.

Appendix L

Recovery of Lost Data and Software

Lost data and software will usually be recovered by a network administrator from the SAN or backup tapes. If the data needed is no longer available on the SAN or in the tape drive, Perpetual Storage is contacted and instructed to bring the needed box or boxes (stored monthly). Depending on urgency, it may be delivered on the regular Tuesday morning visit, or for an additional charge, it can be delivered within an hour. Depending on the nature of the loss, the recovery may take a few minutes to several days or months. If a single file is needed and the user has a date of the loss, in most cases the file can be located fairly quickly and restored. If the data loss is larger, in most cases, the most recent full backup would be restored and then any incremental backups up to the date of loss.

In the event of catastrophic loss of data such as in a fire, flood or earthquake, the last full tape backup set would be used and all of the available incremental backups following (either onsite or requested from Perpetual Storage). All data excluding the Windows Directory and the swap file are backed up and should be available for restoration.

The estimated amount of time needed to recover the most current recoverable data in a total data loss situation would probably be several months. If the backup software restores correctly and the catalog files are available, the time would be greatly reduced. This is keeping in mind that tape has a 30% failure rate. If some tapes prove to be unusable, and prior tapes are needed, this would add to recovery time and also lost data.

Recovery of Hardware: The following is an analysis of the time required to restore agency hardware to the state it was in before the disaster. It assumes a worst case scenario in which all hardware within the building, including the entire LAN room has been lost and must be replaced. Estimates of time and costs necessary for a “partial” disaster could be inferred from this information. Depending on the nature of the disaster which caused loss of hardware the activities described below may have to take place in a new or temporary facility.

With the exception of the LAN room the assumption is made that all necessary telecommunications wiring (PBX, data-circuits, wiring panels, and jacks) are in place and functional. If this is not the case additional time (anywhere from a few days to a few weeks) will be needed to install these network components. Qwest could take at least 30 days to install any new circuits. If we were dealing with a large earthquake, outside communications may take much longer to establish than restoration of services within the agency.

Rewiring of the LAN room in order to accommodate pre-disaster hardware would require about 8 hours of work. This assumes assistance from a DTS wiring crew which would help with connections to telecommunications panels and circuits.

Each machine/device which makes up the LAN room component of the network will have to be ordered, reinstalled and configured. We currently have a total of approximately 70 machines/devices. Usually, machines/devices can be ordered and delivered within 7 working days - a large order could take considerably longer. The estimated total elapsed time necessary for recovery of all hardware to its pre-disaster state is highly variable depending on available staff, length of work week, actual time on task, and unforeseen circumstances. There are 7 network staff members available for recovery of LAN room hardware. If 10 servers/devices per day were configured to proper working order, all machines/devices would be completed in 7 days for a total of 15 days with the 7 day machine/device delivery.

In a worst case scenario, all desktop client machines and network printers would also need to be replaced. We currently have 500 desktop machines, 50 network printers, and 30 desktop printers. Usually, machines can be ordered and delivered within 7 working days - a large order could take considerably longer. The estimated total elapsed time necessary for recovery of all hardware to its pre-disaster state is highly variable depending on available staff, length of work week, actual time on task, and unforeseen contingencies. There are 7 network staff members available for recovery of LAN room hardware. If 50 machines per day were configured to proper working order, all machines would be completed in 13 days for a total of 35 days with the 7 day machine delivery and the 15 days server room recovery being the priority.

Of course this timetable could be accelerated through longer hours and/or outside help. Also, unskilled agency staff could be used to help un-box equipment, move it into place, and plug it into power strips.

Appendix M
USOE Standard Software Installations/Non-Approved Software
May 8, 2007

USOE Standard Software Installations

The applications below are standard installations on new and rebuilt machines:

- OS - Microsoft Windows – Current agency supported version
- Mcafee
- Windows Media Player
- RealOne Player
- QuickTime Player
- Macromedia Flash Play
- Java
- Adobe Acrobat
- Microsoft Office
- Microsoft Anti-Spyware
- USOE Custom Software, i.e., Base, Cactus, etc.
- Corel WordPerfect (as needed)

Programming Software –

PowerBuilder
MS SQL Server
MS Visual Studio

USOE Web Editing applications (Installed only on member's of the Web Team's computers)

Macromedia

Dreamweaver
Fireworks
Flash
Flash Paper
Contribute
Freehand (Installed in Graphics and Printing)

The Web Editing Team is allowed to use Firefox as well, for web page testing purposes

Additional Approved Applications – installed on an as needed basis

Notepad+
Print Key
Adobe Flash Media Encoder

Any other software installed on a USOE Computer needs to be approved utilizing the USOE Software Approval Form.

Appendix N

USOE Software Approval Form

September, 2005

Date: _____

Name of requested software: _____

Machine name software will be installed on: _____

Person requesting installation: _____

Department: _____

Phone number: _____

Software Purpose:

_____

_____

_____

_____

Signature of person requesting software: _____

Signature of zone administrator: _____

Signature of supervisor: _____

Signature of Mark Wagstaff: _____

Software license is on file at: _____

Software installed by: _____

Date of installation: _____

Appendix O

Utah State Office of Education
Research Data Disk Request Guidelines

Persons or organizations who wish to use USOE data to conduct research may request the USOE researcher data disk. To obtain the disk:

1. Requests must be submitted in writing and signed by the person conducting the research, indicating sponsoring organization, if any.

2. Formal Institutional Review Board (IRB) approval must be included in the written request for masters or doctoral studies or other university work.

3. Study will benefit USOE in its mission and work or at least has a direct connection to its mission and work.

4. Study must follow appropriate legal and ethical guidelines, including the Family Educational Rights and Privacy Act (FERPA) requirements and matters of confidentiality.

To obtain the USOE Research Data Disk, contact Randy Raphael (add contact information)

Appendix P

Requests for Other Employee's Data

July 18, 2006

Request Process: In the event data is needed from a retired, terminated or absent employee's H drive, email etc., the following steps should be taken:

- The director or coordinator of the employee's section should clearly outline in writing the file/s needed and the location of the file/s.
- A Help Box Ticket should be submitted outlining the data request. If the Help Box ticket is not submitted by the director or coordinator, the written approval should be emailed to the assigned analyst or attached to the Help Box Ticket.
- The analyst will then provide the director or coordinator with access to the requested file/s.
- Every attempt should be made to coordinate with the employee before retirement, termination (if possible), and absences from the office, in order to identify data that may be needed.

Local Machines: In the event an employee has retired, been terminated, or is absent from the office, time should not be spent locating file/s on the employee's hard drive/s. When an employee retires or is terminated, their local hard drive/s will be wiped. ***It is against USOE Agency Acceptable Use Policy to store work related data on local machines except for incidental and temporary use. Personal or other sensitive data should never be stored on a local machine or peripheral device.***

Network Data: When an employee retires or is terminated, their H drive will be moved to a 'holding' directory for 60 days. If a request has not been submitted following the above outlined Request Process, the H drive data will be deleted. Mail box data will also be kept for 60 days and then deleted if a request for the data has not been submitted.

Protection of Data: Once access to the requested data is provided to the director or coordinator, it will be his or her responsibility to sort through the data to determine which data are appropriate to release.

Appendix Q

Utah State Office of Education

Information Technology Inappropriate Use

Guidelines for Disciplinary Action

The following are guidelines that will be considered by Human Resources when recommending possible disciplinary or other action for inappropriate use of State computers or not complying with the **USOE Confidentiality Agreement and Acceptable Use Policy,** **http://www.schools.utah.gov/computerservices/Policies/USOEConfAgrmntAUP.pdf**. These guidelines are an aid to determine appropriate action by management; they are not intended to be a policy or rule, since each situation is unique and may need to be treated differently. Where the pronoun "he" is used, it is intended to be gender neutral. The State Information Technology policy provides additional guidance on use of these resources. "Inappropriate use" for purpose of this guideline may include viewing, receiving, or sending images, statements, or other material that may be considered to be offensive to others.

Factors to Consider in Determining Appropriate Level of Discipline

- How much time has the employee taken away from his job duties to participate in inappropriate activities? Did these activities or images make reference to employees' race, religion, sex, color, national origin, or disability?
- Did the employee in question only view the inappropriate content or did co-workers inadvertently see them.
- Did the employee freely share inappropriate content with others, thus contributing to their wasting time, etc?
- How inappropriate were the image that were viewed? For example: sexual statements only, soft pornography, hard pornography, children, etc. Note: If any children are involved, we are required to contact law enforcement officials.
- Did the employee freely, accidentally, or by not complying with security policy directives, expose or share confidential or protected data (student, teacher & employee records) with others, thus contributing to FERPA or GRAMA violation(s).
- Does the employee have a position of trust? This may include IT professionals, supervisory and management employees, and others in positions of trust. Employees in these positions may be judged against a higher standard, than those in less responsible positions.
- Is this a new employee who is in his probationary period?
- Did the employee attempt to hide or cover-up his involvement in the inappropriate activity?
- Is this a repeat offense? If so, how long has it been since the prior situation?
- Are there other factors that should be considered in this specific instance?

Considerations for Discipline

When should management not take any formal action?	• There was no verification of inappropriate action.
When should a **Verbal Warning** be considered?	• The employee was not directly involved. • It was a first offense. • There was no impact on others.
When should a **Written Warning or Written Reprimand** be considered? *(Only one of these considerations needs to be met.)*	• This is a first time offense and the content of material is not pornographic. • The amount of time spent on this inappropriate activity is minimal. • Co-workers were not inadvertently subjected to inappropriate images. • The material was not shared extensively with other willing participants. • The shared or exposed confidential data were of very small volume and not highly exposed
When should a **Suspension** be considered? *(Only one of these considerations needs to be met.)*	• This is a first time offense and the content of material is pornographic. • The amount of time spent on this inappropriate activity is extensive. • Co-workers were inadvertently subjected to inappropriate images. • The material was repeatedly shared with other willing participants. • The shared or exposed confidential data were of large volume and/or highly exposed.
Factors to determine length of **Suspension**	• How much time did the employee spend on inappropriate activities. • How much potential liability has the employee's inappropriate actions caused the organization? • How extensive was the inappropriate activities. • How many others were involved in it?
When should **Termination** for the first offense be considered? *(Only one of these considerations needs to be met.)*	• When the employee is in a position of trust, and the confidence in the employee has been eroded to the point that he can no longer function in his position. • When there has been extensive involvement in pornography. • When the inappropriate activities have involved children, solicitation in chat rooms, or similar actions. • If the employee is in a probationary status, do mitigating

reason exist to retain the employee?

When should a **Termination** be considered on a 2nd or subsequent offense? *(Only one of these considerations needs to be met.)*

- If the behavior continued after receiving prior discipline for the same, or similar inappropriate actions.
- If the liability to the organization increased due to the repeat nature of the infraction.
- If the person, irrespective of position, has lost the trust of leaders to the point that he can no longer function in his position.
- A mitigating factor may be if there was a repeat violation, but it was minor, did not involve others, and there was a significant amount of time between infractions.
- If the employee is not terminated on the second offense, he should receive a notice that any repeat violations will very likely result in termination of employment.

Appendix R

Researcher Confidentiality and Use Agreement Regarding Microdata

Microdata means data about individual persons. In the context of education, it specifically means data about individual students and educators. In the context of educational research, use of microdata entails regarding the students and educators in question as human subjects entitled to all protections afforded by the ethical practice of science.

Confidentiality is one such practice. Confidentiality means managing personal information a subject has disclosed in a relationship of trust (for example, to obtain educational services or employment) in a way that protects the identity of the subject from inappropriate redisclosure and thus the subject from any potential harm that inappropriate use of microdata might cause. In the context of anonymized or deidentified data, confidentiality also implies that no effort will be made by the researcher to discover the identity of a subject.

I hereby affirm that I will maintain as strictly confidential microdata made available to me for research purposes by the Utah State Office of Education (USOE) and will not use the microdata for any purpose other than research. I will notify the USOE within 24 hours of any suspected violation of confidentiality, whether mine or anyone else's, whether intentional or accidental. I understand that a violation of this pledge will result in a material breach of contract and may subject me and the organization for which I work to prosecution under applicable laws.

I promise to provide the USOE with a copy of any published report I write based on research utilizing microdata I have obtained under this agreement. I understand that the USOE may publish annotated bibliographic information about my work but will not reproduce the report itself for distribution outside of the USOE without express written permission from the copyright holder.

If I receive personally identifiable information under commission by the USOE to perform research on its behalf, I will also strictly adhere to all additional relevant provisions of the confidentiality agreement set out in **Appendix I** for USOE employees.

_____
Name of Principal Investigator (please print)

_____
Organizational Affiliation

_____
Email Address

_____
Phone Number

_____
Signature of Principal Investigator

_____
Date